

1 TO THE HONORABLE SENATE:

2 The Committee on Government Operations to which was referred House
3 Bill No. 291 entitled “An act relating to creation of a cybersecurity task force”
4 respectfully reports that it has considered the same and recommends that the
5 Senate propose to the House that the bill be amended by striking out all after
6 the enacting clause and inserting in lieu thereof the following:

7 Sec. 1. 20 V.S.A. chapter 208 is added to read:

8 CHAPTER 208. CYBERSECURITY

9 § 4661. DEFINITIONS

10 As used in this chapter:

11 (1) “Critical infrastructure” has the same meaning as in 11 V.S.A.

12 § 1701.

13 (2) “Cybersecurity” means the practice of deploying people, policies,
14 processes, and technologies to protect organizations, their critical systems, and
15 sensitive information from digital attacks.

16 (3) “Essential supply chain” supply chains for the production, in
17 sufficient quantities, of the following articles:

18 (A) medical supplies, medicines, and personal protective equipment;

19 (B) articles essential to the operation, manufacture, supply, service,

20 or maintenance of critical infrastructure;

1 (C) articles critical to infrastructure construction after a natural or
2 manmade disaster;

3 (D) articles that are critical to the State’s food systems, including
4 food supplies for individuals and households and livestock feed; and

5 (E) any other articles identified in [rules or by a specific department
6 or person?]

7 § 4662. CYBERSECURITY ADVISORY COUNCIL

8 (a) Creation. There is created the Cybersecurity Advisory Council to
9 advise on the State’s cybersecurity infrastructure, best practices,
10 communications protocols, standards, training, and safeguards.

11 (b) Membership. The Council shall be composed of the following
12 members:

13 (1) one current member of the House of Representatives, who shall be
14 appointed by the Speaker of the House;

15 (2) one current member of the Senate, who shall be appointed by the
16 Committee on Committees;

17 (3) the Chief Information Officer, who shall serve as the Chair or
18 appoint a designee from the Council to serve as the Chair;

19 (4) the Chief Information Security Officer;

20 (5) a representative from a State electrical public utility, appointed by
21 the Commissioner of Public Service;

1 (6) a representative from a State municipal water system, appointed by
2 the Green Mountain Water Environment Association [OR Secretary of Natural
3 Resources];

4 (7) a representative from a Vermont hospital organization, appointed by
5 the President of the Vermont Association of Hospitals and Health Systems;

6 (8) a person representing a Vermont business related to an essential
7 supply chain, appointed by the Chair of the Vermont Business Roundtable;

8 (9) the Director of Vermont Emergency Management or designee;

9 (10) the Governor’s Homeland Security Advisor or designee;

10 (11) the Vermont Adjutant General or designee;

11 (12) the Attorney General or designee; and

12 (13) the President of Vermont Information Technology Leaders or
13 designee.

14 (c) Powers and duties. The Council shall have the following duties:

15 (1) develop a strategic plan for protecting the State’s public sector and
16 private sector information and systems from cybersecurity attacks;

17 (2) review and approve the State’s cybersecurity standards for critical
18 infrastructure domains;

19 (3) evaluate statewide cybersecurity readiness and develop and share
20 best practices for policies and procedures to strengthen administrative,

1 technical, and physical cybersecurity safeguards as a resource for State
2 government, Vermont businesses, and the public;

3 (4) build relationships and conduct outreach within State government
4 and to federal government and the private sector to ensure the resilience of
5 electronic information systems;

6 (5) build strong partnerships with local universities and colleges in order
7 to leverage cybersecurity resources; and

8 (6) conduct an inventory and review of cybersecurity standards for
9 critical sector infrastructures and make recommendations on whether improved
10 or additional standards are necessary; and

11 (7) identify and advise on opportunities to:

12 (A) ensure Vermont promotes, attracts, and retains a highly skilled
13 cybersecurity workforce;

14 (B) raise citizen awareness through outreach and public service
15 announcements;

16 (C) provide technical capabilities, training, and advice to local
17 government and the private sector;

18 (D) provide recommendations on legislative action to the General
19 Assembly to protect critical assets, infrastructure, services, and personally
20 identifiable information;

1 (E) advise on strategic, operational, and budgetary impacts of
2 cybersecurity on the State;

3 (F) engage State and federal partners in assessing and managing risk;

4 (G) investigate ways the State can implement a unified cybersecurity
5 communications and response, including recommendations for building a
6 Statewide communication network in the event of a cybersecurity emergency;

7 (H) relating to cyber-insurance, including how to increase availability
8 and affordability of cyber-insurance for critical industries.

9 (d) Assistance. The Council shall have the administrative and technical
10 assistance of the Agency of Digital Services.

11 (e) Working groups and consultations.

12 (1) The Council may establish interagency working groups to support its
13 charge, drawing membership from any State agency or department.

14 (2) The Council may consult with private sector and municipal, State,
15 and federal government professionals for information and advice on issues
16 related to the Council's charge.

17 (f) Meetings.

18 ~~(1) The Chief Information Officer shall be the Chair of the Council.~~

19 (1) A majority of the membership shall constitute a quorum.

20 (2) The Council shall meet at least quarterly.

1 (g) Reports. On or before January 15 each year, the Council shall submit a
2 written report to the House Committees on Commerce and Economic
3 Development, on Environment and Energy, on Government Operations and
4 Military Affairs, and on Ways and Means and the Senate Committees on
5 Economic Development, Housing and General Affairs, on Finance, and on
6 Government Operations with a status update on the work of the Council and
7 any recommendations for legislative action. The provisions of 2 V.S.A. §
8 20(d) (expiration of required reports) shall not apply to the report to be made
9 under this subsection.

10 (h) Compensation and reimbursement.

11 (1) For attendance at meetings during adjournment of the General
12 Assembly, a legislative member of the Council serving in the member's
13 capacity as a legislator shall be entitled to per diem compensation and
14 reimbursement of expenses pursuant to 2 V.S.A. § 23. These payments shall
15 be made from monies appropriated to the General Assembly.

16 (2) Other members of the Council who are not otherwise compensated
17 or reimbursed for their attendance shall be entitled to per diem compensation
18 and reimbursement of expenses as permitted under 32 V.S.A. § 1010. These
19 payments shall be made from monies appropriated to the Agency of Digital
20 Services.

21 Sec. 2. 11 V.S.A. § 1701 is amended to read:

1 § 1701. DEFINITIONS

2 ~~In~~ As used in this chapter:

3 (1) “Critical infrastructure” means property and equipment owned or
4 used by communications networks and electric generation, transmission, and
5 distribution systems; water and wastewater systems; health systems; essential
6 supply chains; and communications networks, including cellular, broadband,
7 and telecommunications networks.

8 * * *

9 Sec. 3. REPEAL

10 20 V.S.A. chapter 208 (cybersecurity) is repealed on June 30, 2028.

11 Sec. 4. EFFECTIVE DATE

12 This act shall take effect on July 1, 2023.

13

14

15

16

17

18 (Committee vote: _____)

19

20

21

Senator _____

FOR THE COMMITTEE